FIG. 1

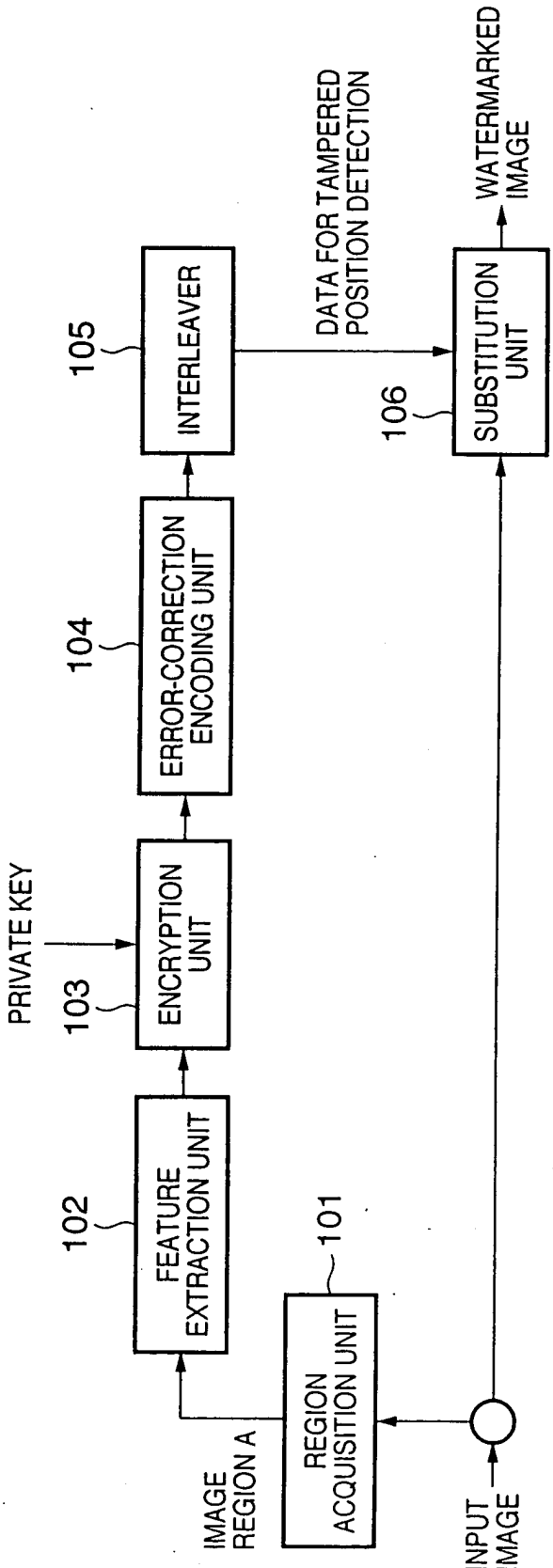

INPUT IMAGE
IMAGE REGION A
REGION ACQUISITION UNIT
101
FEATURE EXTRACTION UNIT
102
PRIVATE KEY
ENCRYPTION UNIT
103
ERROR-CORRECTION ENCODING UNIT
104
INTERLEAVER
105
DATA FOR TAMPERED POSITION DETECTION
SUBSTITUTION UNIT
106
WATERMARKED IMAGE

FIG. 2

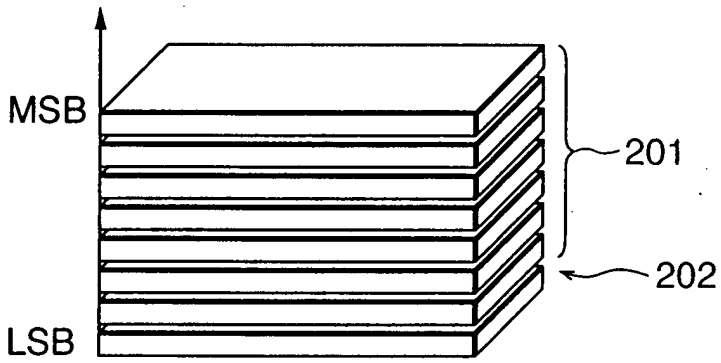
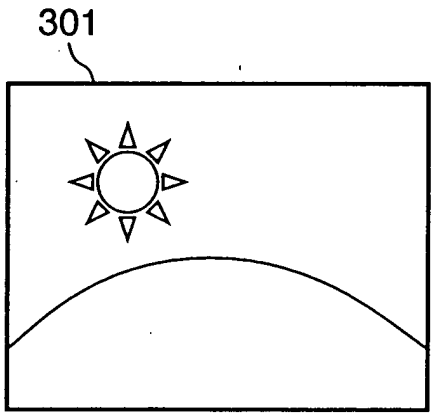
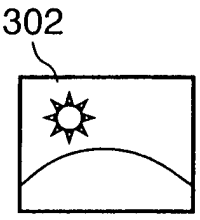


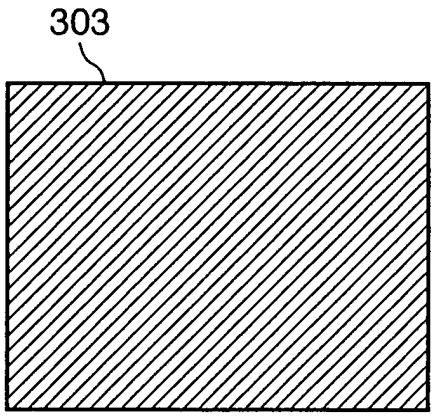
FIG. 3



INPUT IMAGE
(MULTI-VALUE)



2D FEATURE IMAGE
(BINARY)



RANDOMIZED, ERROR-CORRECTION ENCODED,
ENCRYPTED WATERMARK INFORMATION
(BINARY)

FIG. 4

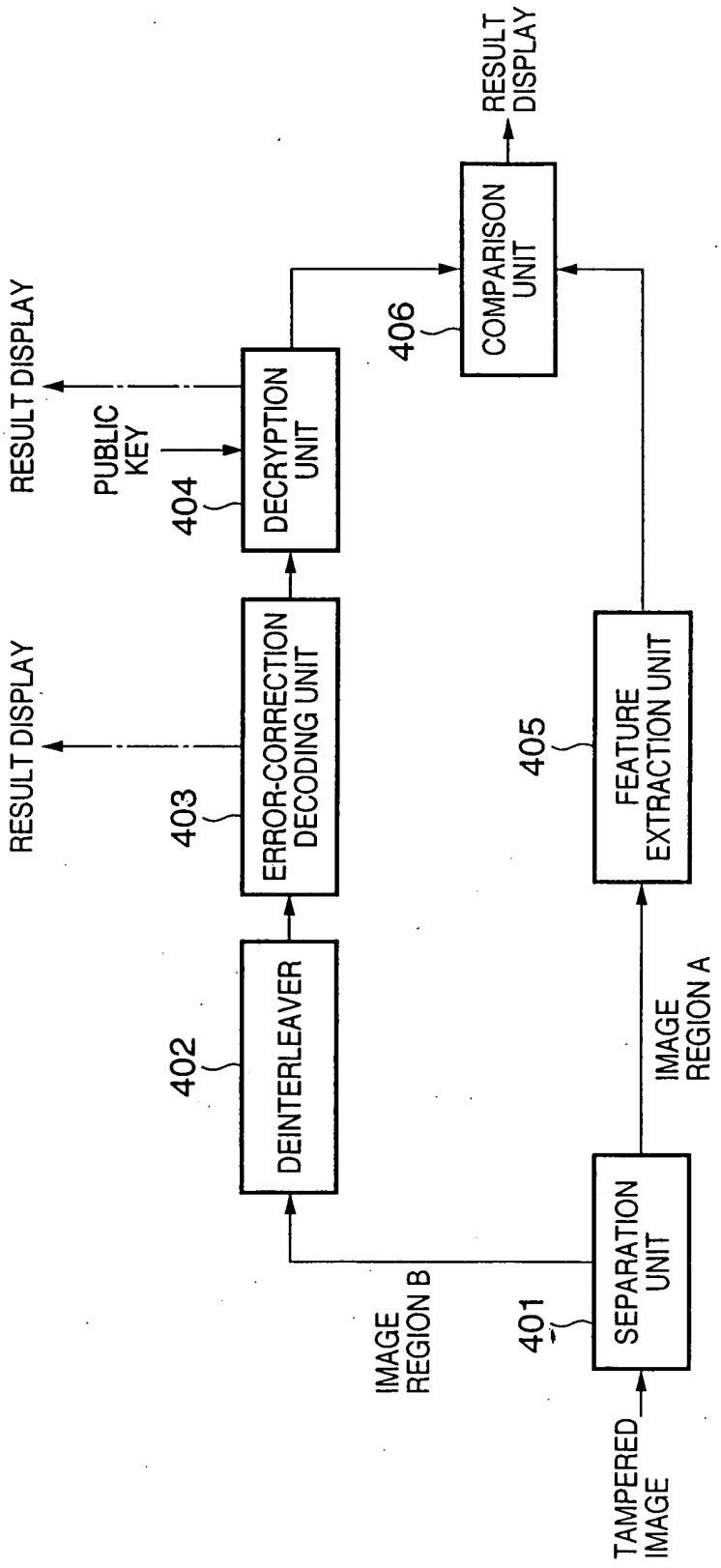

TAMPERED IMAGE
401
SEPARATION UNIT
IMAGE REGION A
IMAGE REGION B
402
DEINTERLEAVER
403
ERROR-CORRECTION DECODING UNIT
RESULT DISPLAY
404
PUBLIC KEY
DECRYPTION UNIT
RESULT DISPLAY
405
FEATURE EXTRACTION UNIT
406
COMPARISON UNIT
RESULT DISPLAY

FIG. 5

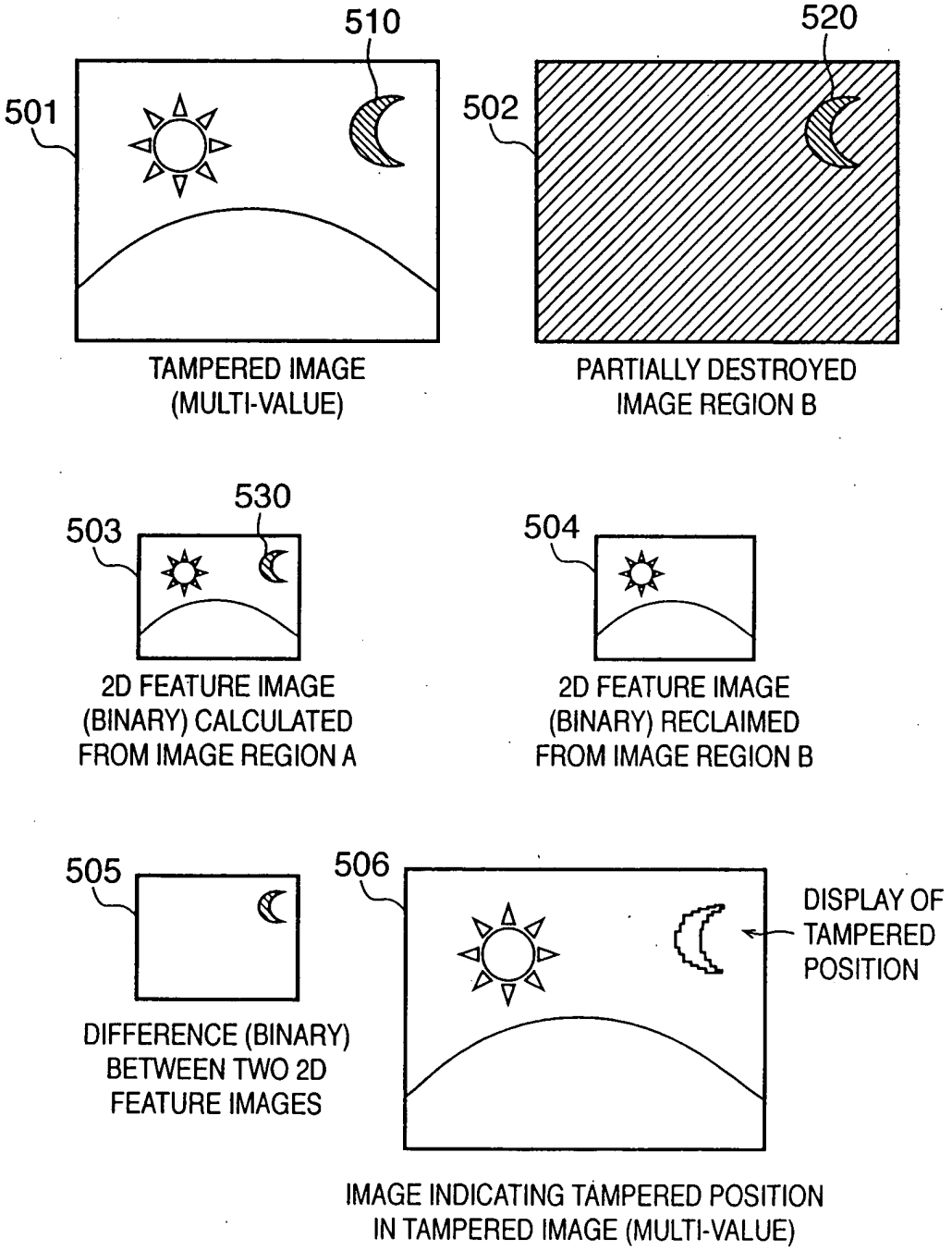

510
501
TAMPERED IMAGE
(MULTI-VALUE)
520
502
PARTIALLY DESTROYED
IMAGE REGION B
530
503
2D FEATURE IMAGE
(BINARY) CALCULATED
FROM IMAGE REGION A
504
2D FEATURE IMAGE
(BINARY) RECLAIMED
FROM IMAGE REGION B
505
DIFFERENCE (BINARY)
BETWEEN TWO 2D
FEATURE IMAGES
506
DISPLAY OF
TAMPERED
POSITION
IMAGE INDICATING TAMPERED POSITION
IN TAMPERED IMAGE (MULTI-VALUE)

FIG. 6

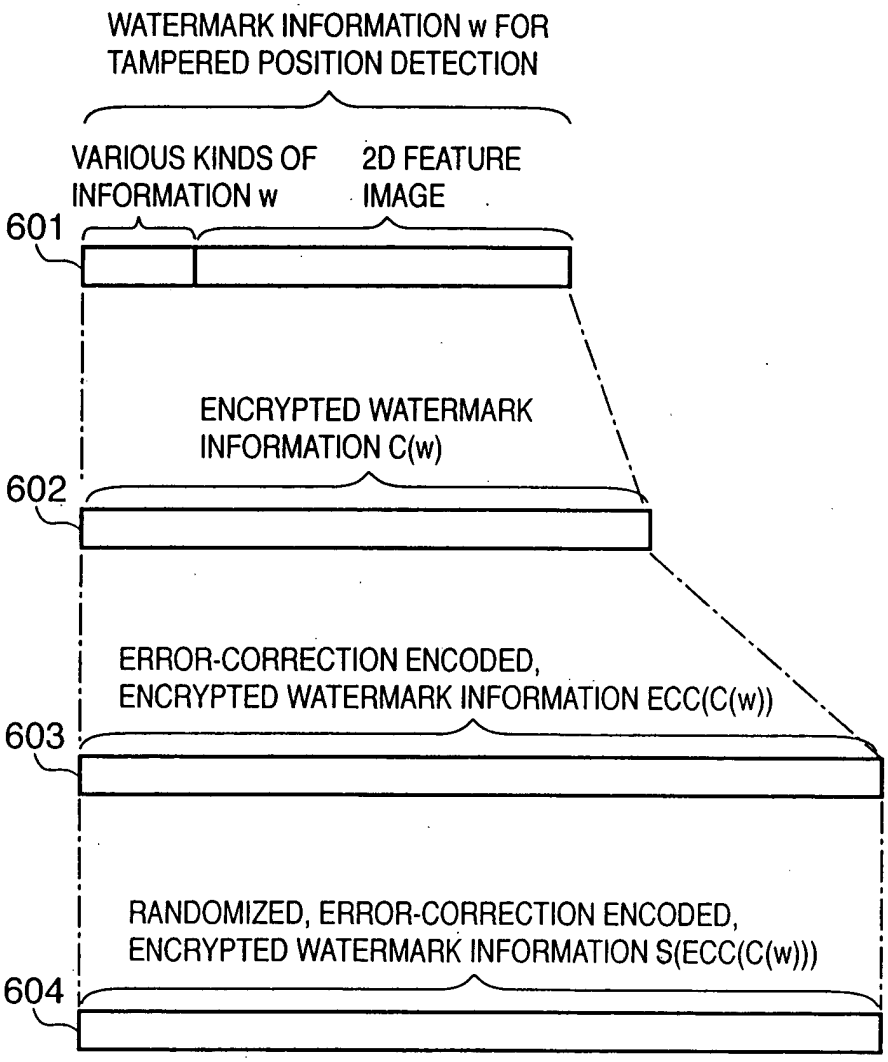

WATERMARK INFORMATION w FOR TAMPERED POSITION DETECTION
VARIOUS KINDS OF INFORMATION w
2D FEATURE IMAGE
601
ENCRYPTED WATERMARK INFORMATION C(w)
602
ERROR-CORRECTION ENCODED, ENCRYPTED WATERMARK INFORMATION ECC(C(w))
603
RANDOMIZED, ERROR-CORRECTION ENCODED, ENCRYPTED WATERMARK INFORMATION S(ECC(C(w)))
604

FIG. 7

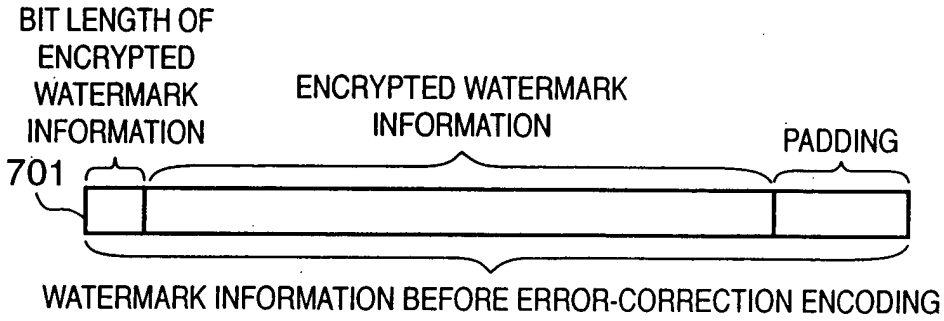

BIT LENGTH OF ENCRYPTED WATERMARK INFORMATION
ENCRYPTED WATERMARK INFORMATION
PADDING
701
WATERMARK INFORMATION BEFORE ERROR-CORRECTION ENCODING

FIG. 8

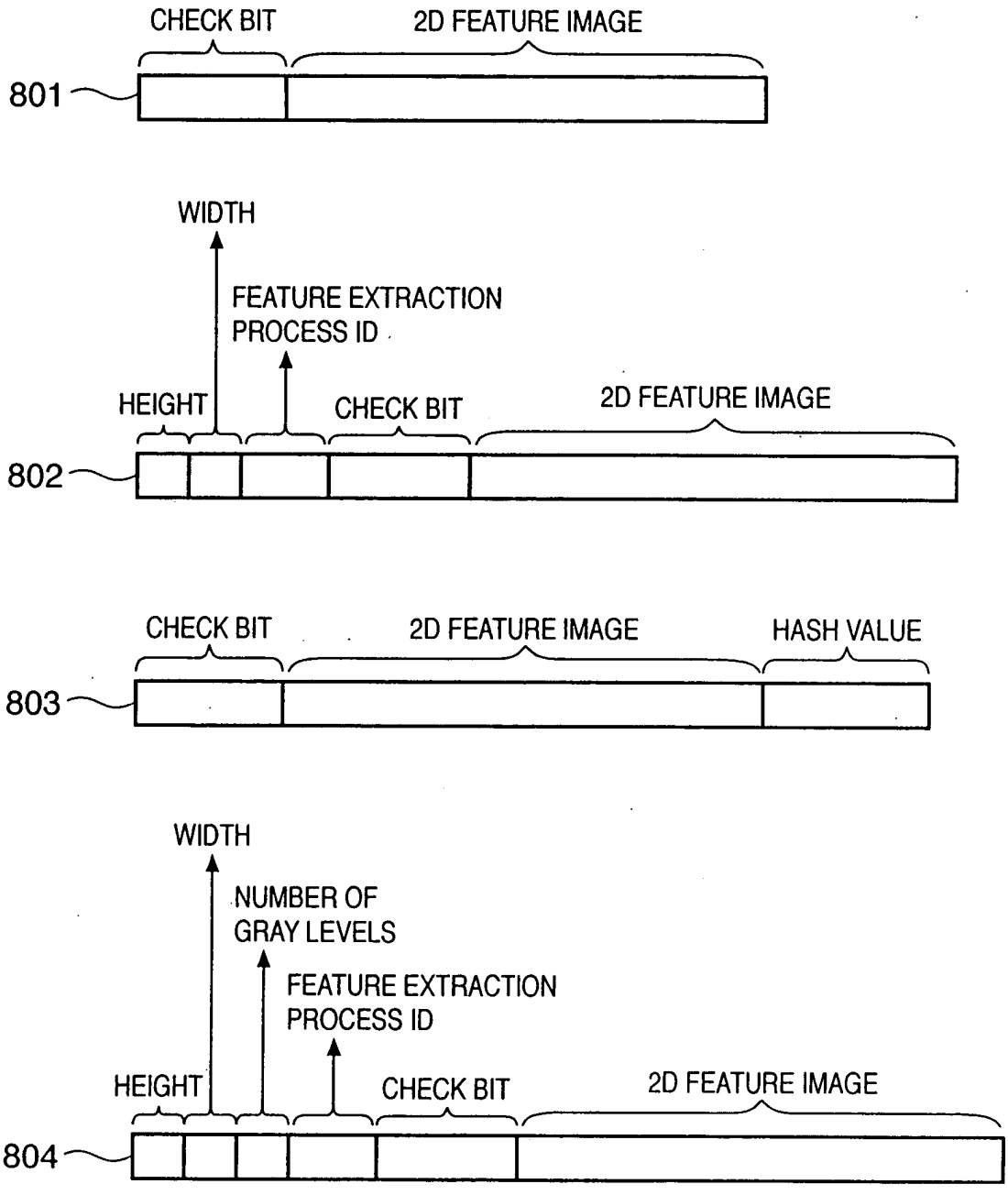

CHECK BIT
2D FEATURE IMAGE
801
WIDTH
FEATURE EXTRACTION PROCESS ID
HEIGHT
CHECK BIT
2D FEATURE IMAGE
802
CHECK BIT
2D FEATURE IMAGE
HASH VALUE
803
WIDTH
NUMBER OF GRAY LEVELS
FEATURE EXTRACTION PROCESS ID
HEIGHT
CHECK BIT
2D FEATURE IMAGE
804

FIG. 9

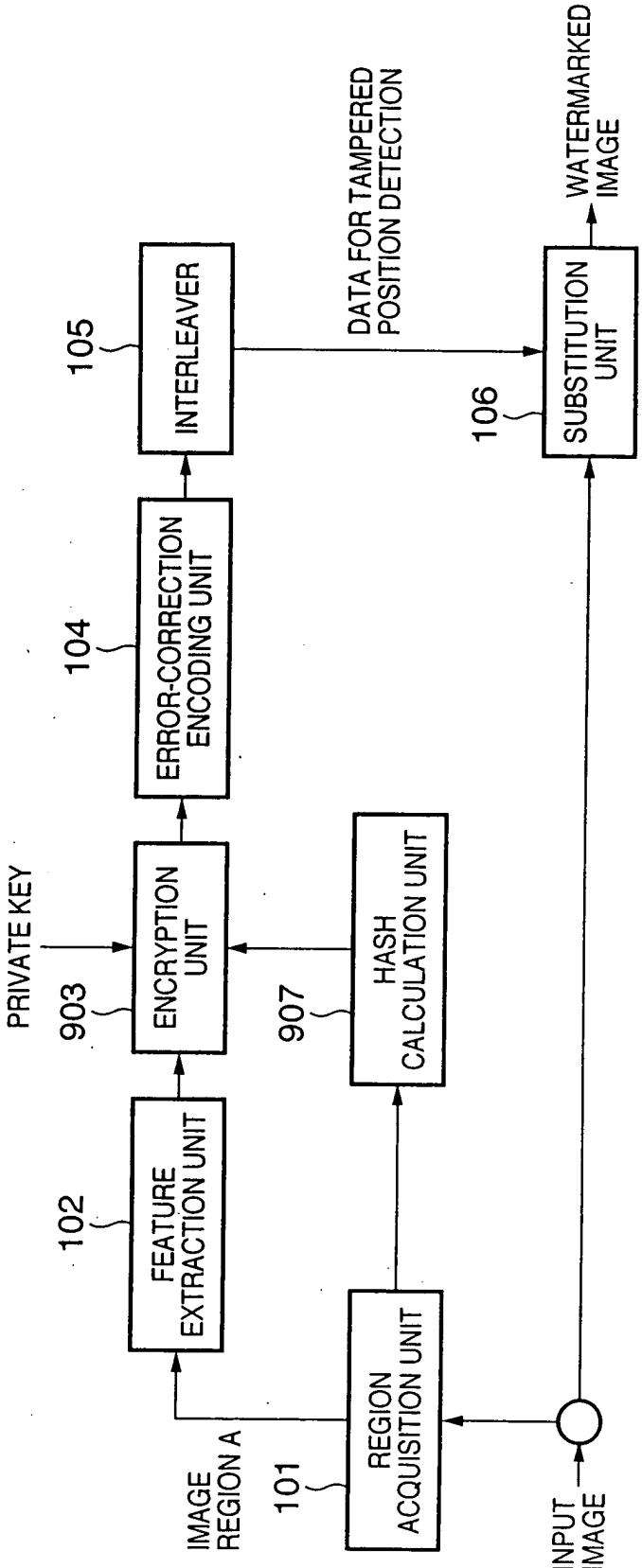

INPUT IMAGE
IMAGE REGION A
101
REGION ACQUISITION UNIT
102
FEATURE EXTRACTION UNIT
907
HASH CALCULATION UNIT
PRIVATE KEY
903
ENCRYPTION UNIT
104
ERROR-CORRECTION ENCODING UNIT
105
INTERLEAVER
DATA FOR TAMPERED POSITION DETECTION
106
SUBSTITUTION UNIT
WATERMARKED IMAGE

FIG. 10

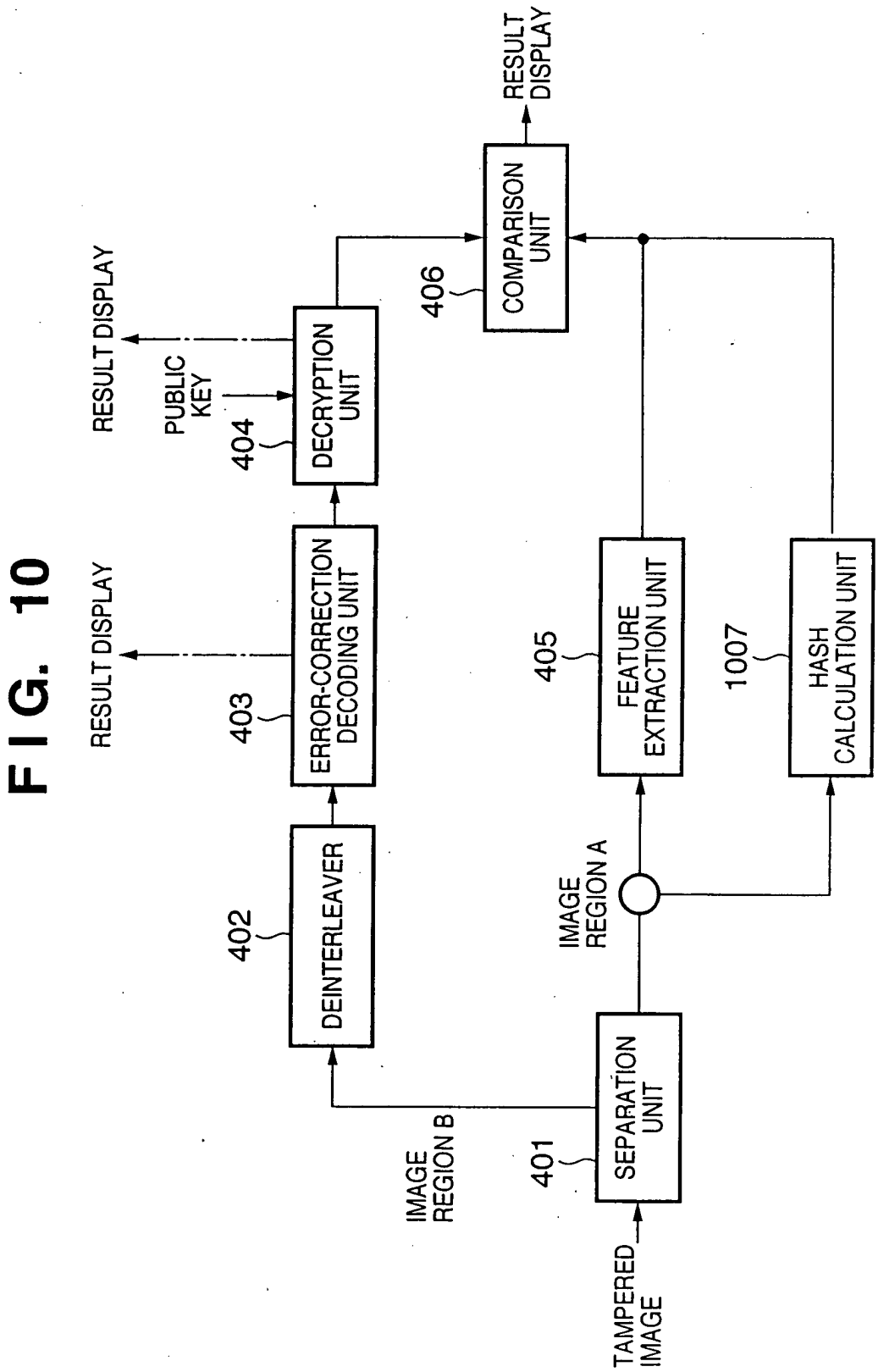

TAMPERED IMAGE
401
SEPARATION UNIT
IMAGE REGION B
IMAGE REGION A
402
DEINTERLEAVER
403
ERROR-CORRECTION DECODING UNIT
RESULT DISPLAY
404
PUBLIC KEY
DECRYPTION UNIT
RESULT DISPLAY
405
FEATURE EXTRACTION UNIT
1007
HASH CALCULATION UNIT
406
COMPARISON UNIT
RESULT DISPLAY

FIG. 11

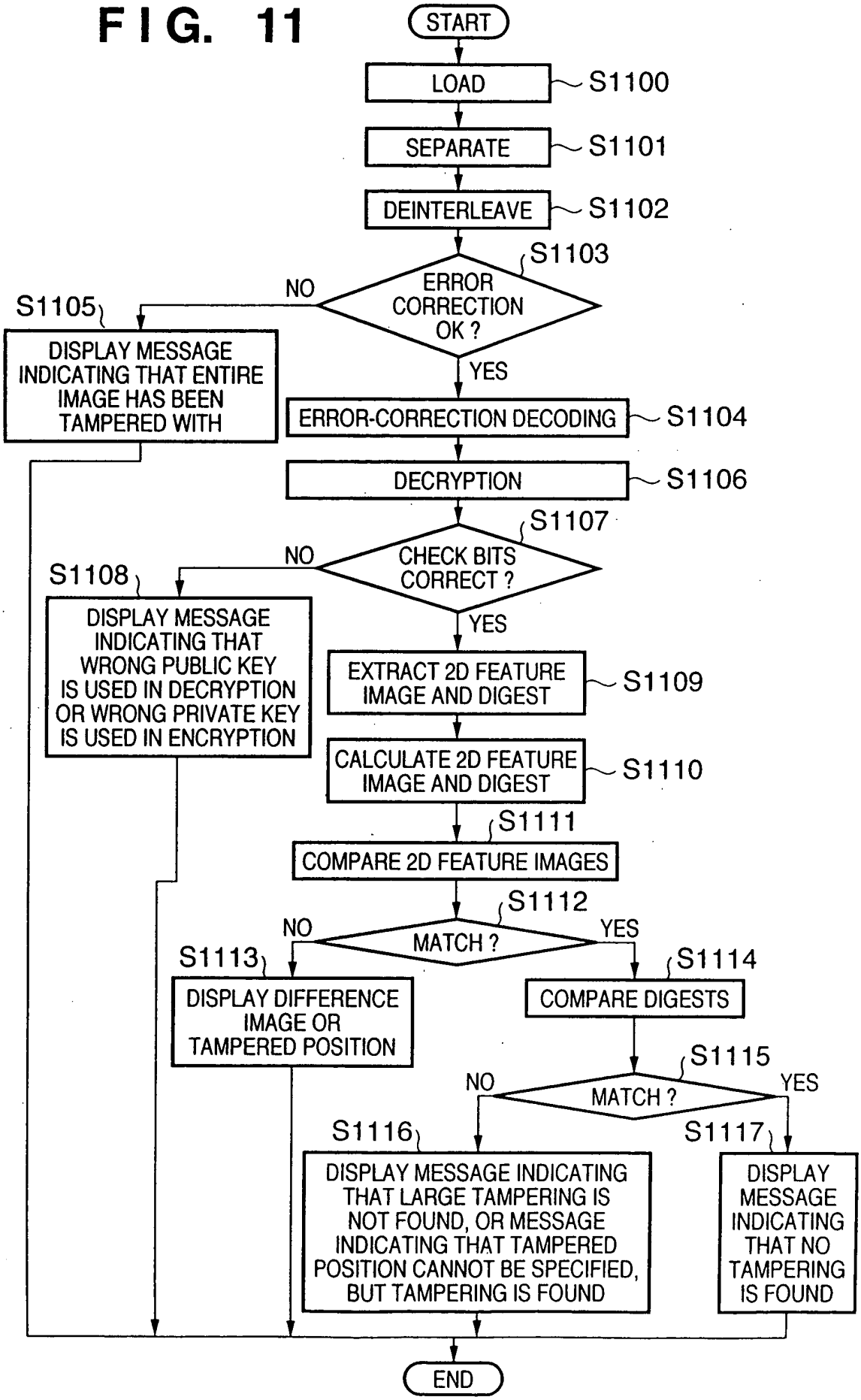

START
LOAD
S1100
SEPARATE
S1101
DEINTERLEAVE
S1102
S1103
ERROR CORRECTION OK ?
NO
YES
S1105
DISPLAY MESSAGE INDICATING THAT ENTIRE IMAGE HAS BEEN TAMPERED WITH
ERROR-CORRECTION DECODING
S1104
DECRYPTION
S1106
S1107
CHECK BITS CORRECT ?
NO
YES
S1108
DISPLAY MESSAGE INDICATING THAT WRONG PUBLIC KEY IS USED IN DECRYPTION OR WRONG PRIVATE KEY IS USED IN ENCRYPTION
EXTRACT 2D FEATURE IMAGE AND DIGEST
S1109
CALCULATE 2D FEATURE IMAGE AND DIGEST
S1110
S1111
COMPARE 2D FEATURE IMAGES
S1112
MATCH ?
NO
YES
S1113
DISPLAY DIFFERENCE IMAGE OR TAMPERED POSITION
S1114
COMPARE DIGESTS
S1115
MATCH ?
NO
YES
S1116
DISPLAY MESSAGE INDICATING THAT LARGE TAMPERING IS NOT FOUND, OR MESSAGE INDICATING THAT TAMPERED POSITION CANNOT BE SPECIFIED, BUT TAMPERING IS FOUND
S1117
DISPLAY MESSAGE INDICATING THAT NO TAMPERING IS FOUND
END

FIG. 12

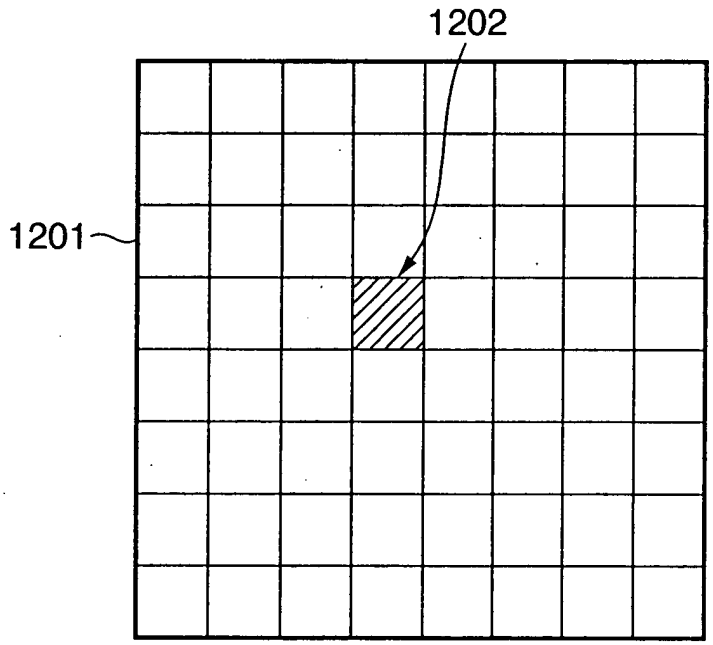


FIG. 13

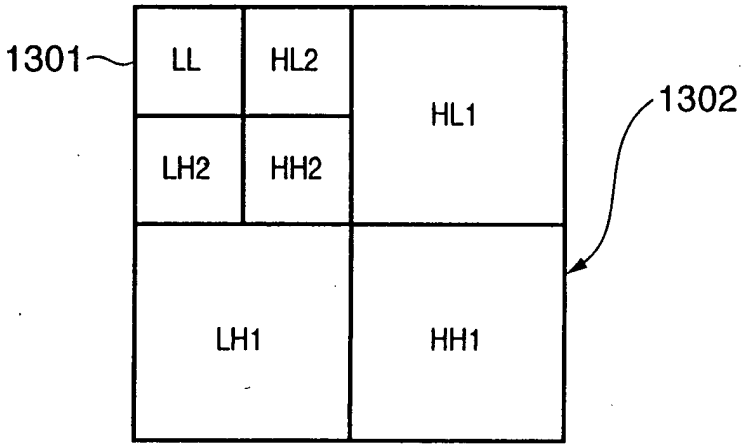


FIG. 14

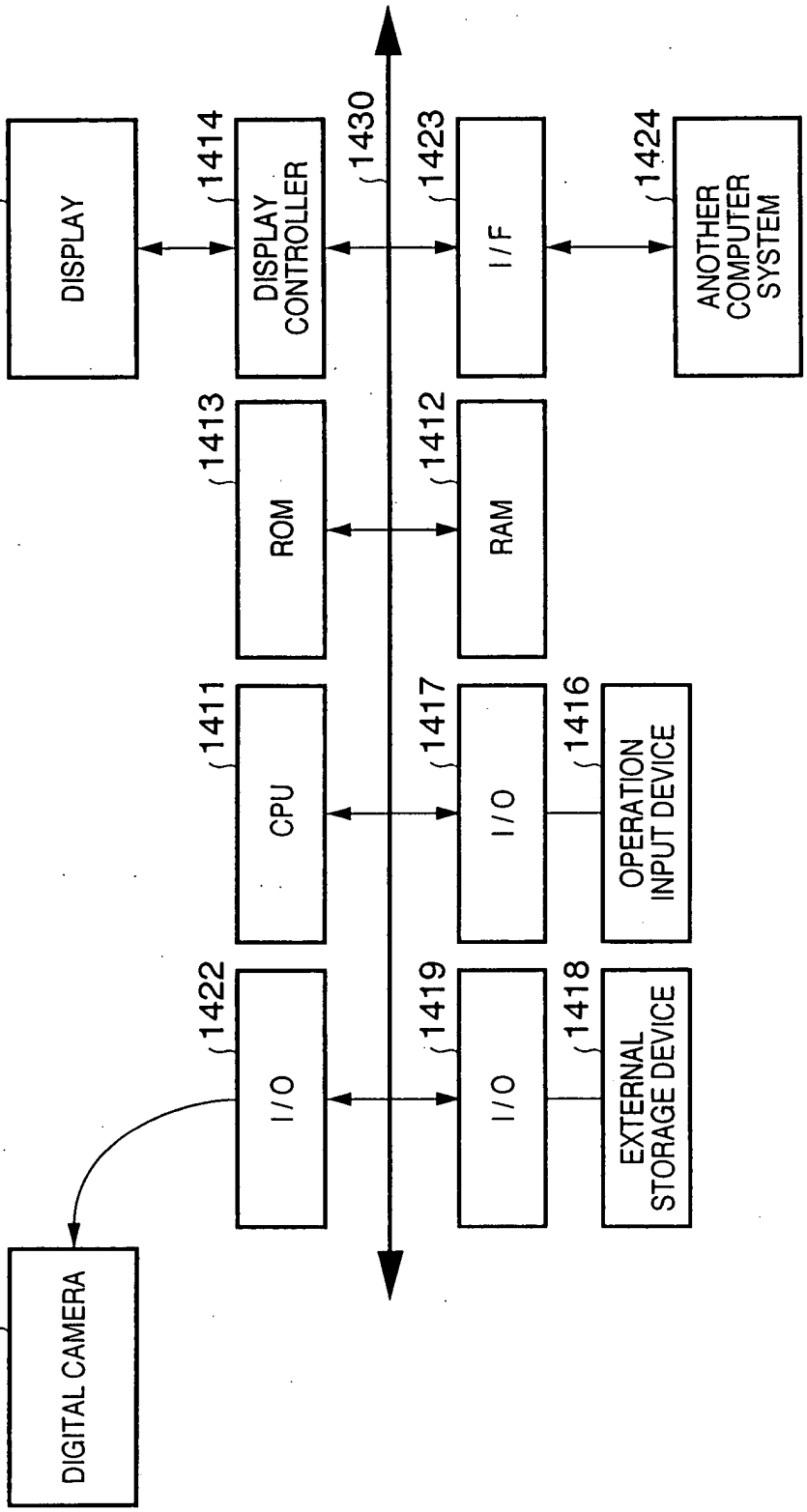

1415
DISPLAY
1414
DISPLAY CONTROLLER
1430
1423
I/F
1424
ANOTHER COMPUTER SYSTEM
1413
ROM
1412
RAM
1411
CPU
1417
I/O
1416
OPERATION INPUT DEVICE
1422
I/O
1419
I/O
1418
EXTERNAL STORAGE DEVICE
1421
DIGITAL CAMERA

FIG. 15

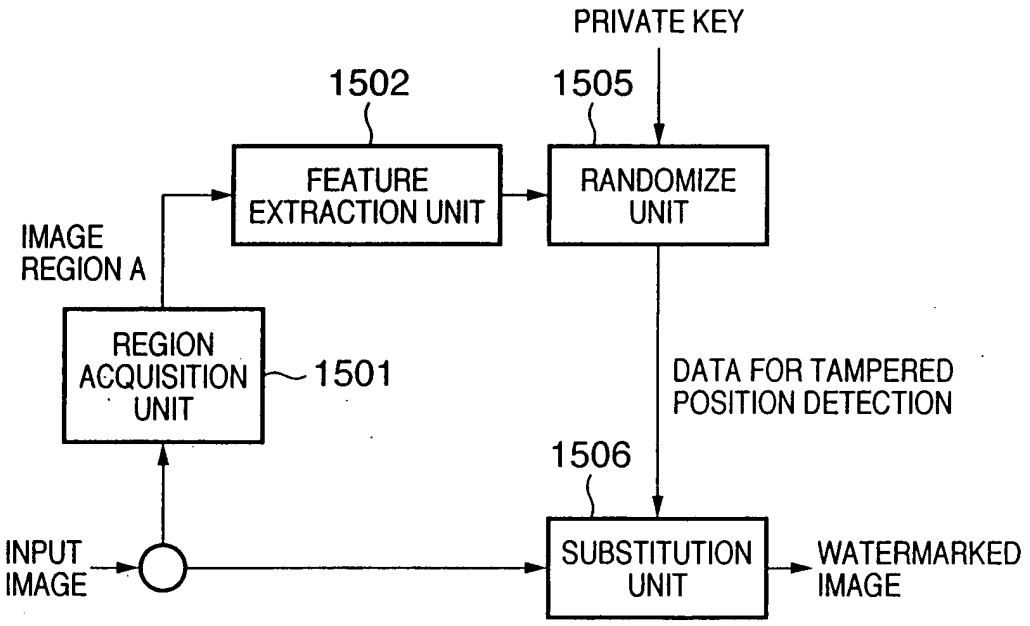

PRIVATE KEY
1502
1505
FEATURE EXTRACTION UNIT
RANDOMIZE UNIT
IMAGE REGION A
REGION ACQUISITION UNIT
1501
DATA FOR TAMPERED POSITION DETECTION
1506
INPUT IMAGE
SUBSTITUTION UNIT
WATERMARKED IMAGE

FIG. 16

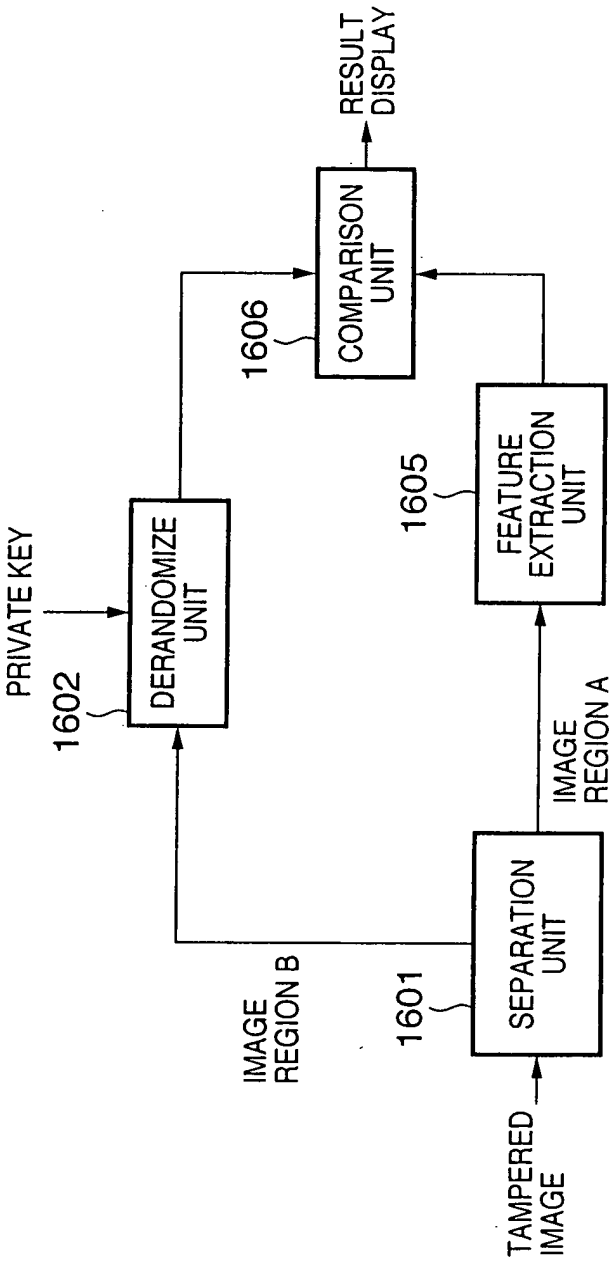

TAMPERED IMAGE
SEPARATION UNIT
1601
IMAGE REGION B
IMAGE REGION A
PRIVATE KEY
DERANDOMIZE UNIT
1602
FEATURE EXTRACTION UNIT
1605
COMPARISON UNIT
1606
RESULT DISPLAY

FIG. 17

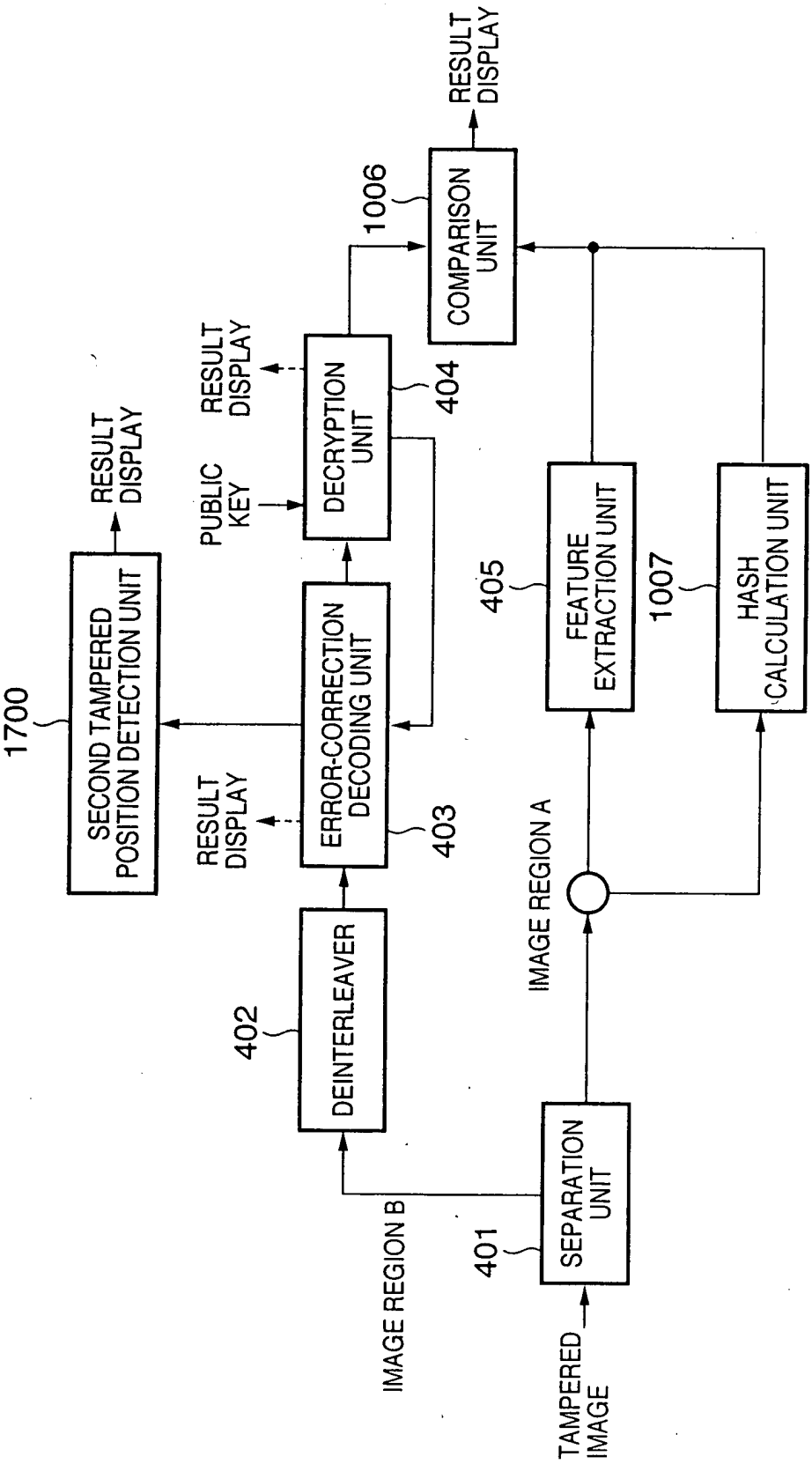

TAMPERED IMAGE
SEPARATION UNIT
401
IMAGE REGION B
IMAGE REGION A
DEINTERLEAVER
402
ERROR-CORRECTION DECODING UNIT
403
DECRYPTION UNIT
404
PUBLIC KEY
FEATURE EXTRACTION UNIT
405
HASH CALCULATION UNIT
1007
COMPARISON UNIT
1006
SECOND TAMPERED POSITION DETECTION UNIT
1700
RESULT DISPLAY
RESULT DISPLAY
RESULT DISPLAY
RESULT DISPLAY

FIG. 18

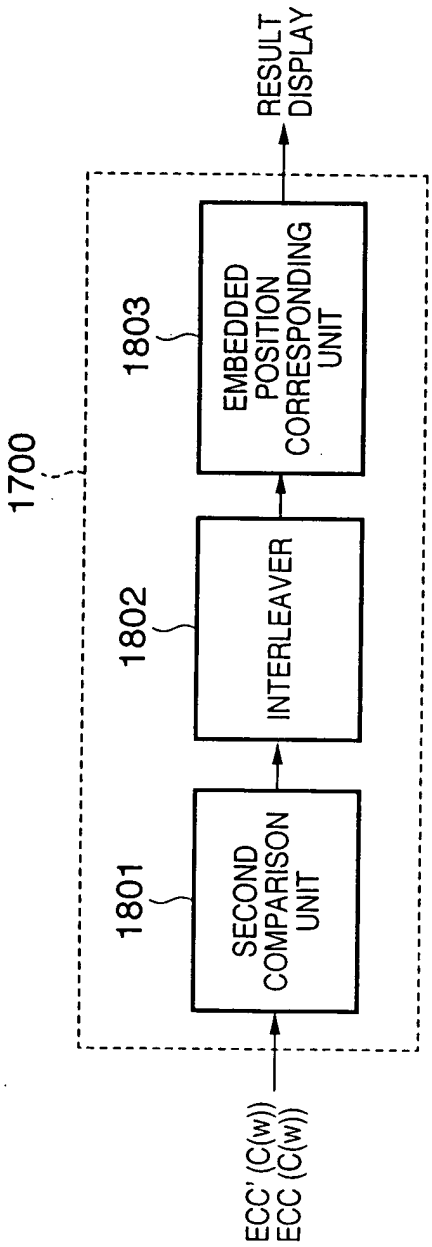

ECC' (C(w))
ECC (C(w))
1700
1801
SECOND COMPARISON UNIT
1802
INTERLEAVER
1803
EMBEDDED POSITION CORRESPONDING UNIT
RESULT DISPLAY

FIG. 19

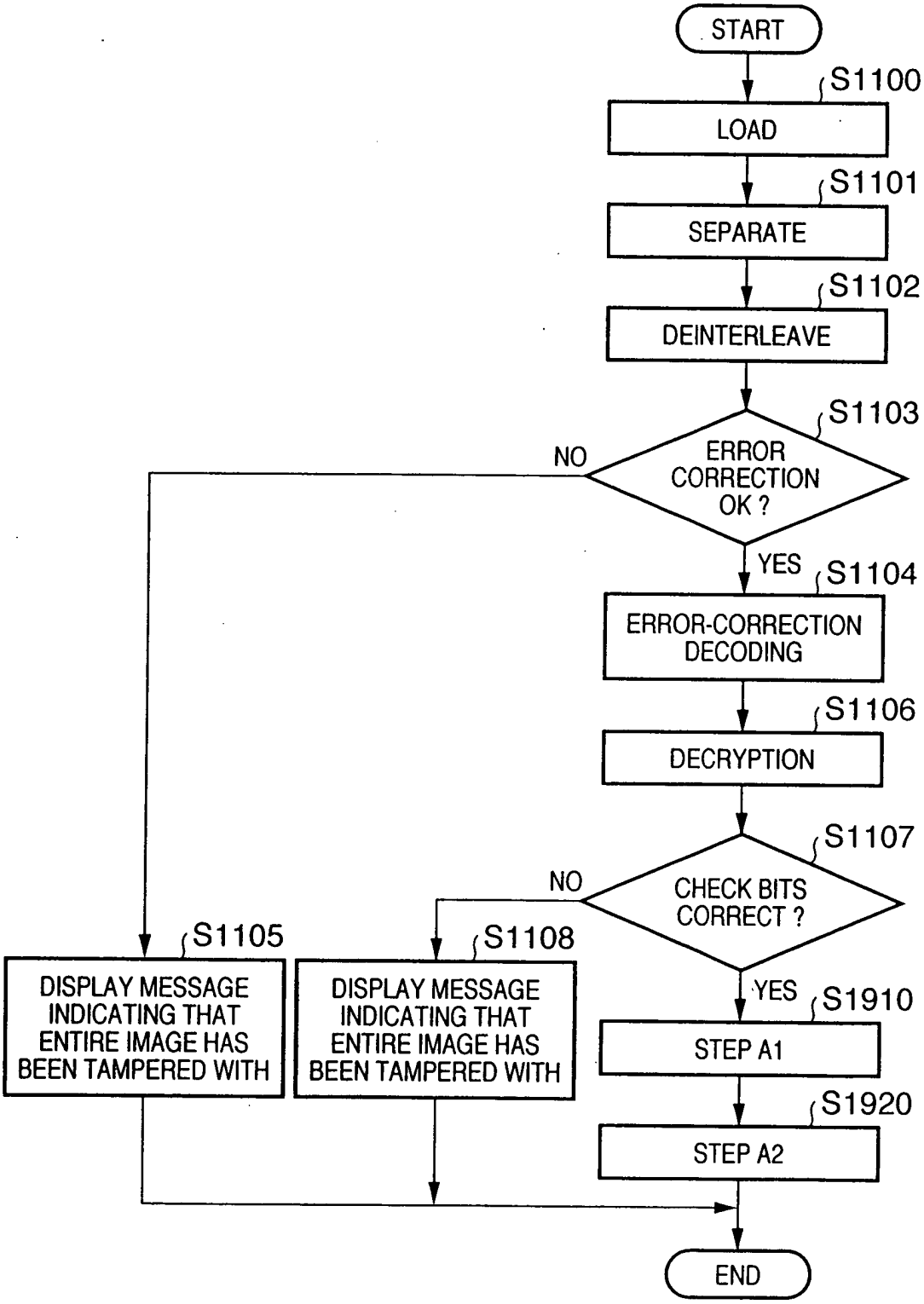

START
S1100
LOAD
S1101
SEPARATE
S1102
DEINTERLEAVE
S1103
ERROR CORRECTION OK ?
NO
YES
S1104
ERROR-CORRECTION DECODING
S1106
DECRYPTION
S1107
CHECK BITS CORRECT ?
NO
YES
S1105
DISPLAY MESSAGE INDICATING THAT ENTIRE IMAGE HAS BEEN TAMPERED WITH
S1108
DISPLAY MESSAGE INDICATING THAT ENTIRE IMAGE HAS BEEN TAMPERED WITH
S1910
STEP A1
S1920
STEP A2
END

FIG. 20

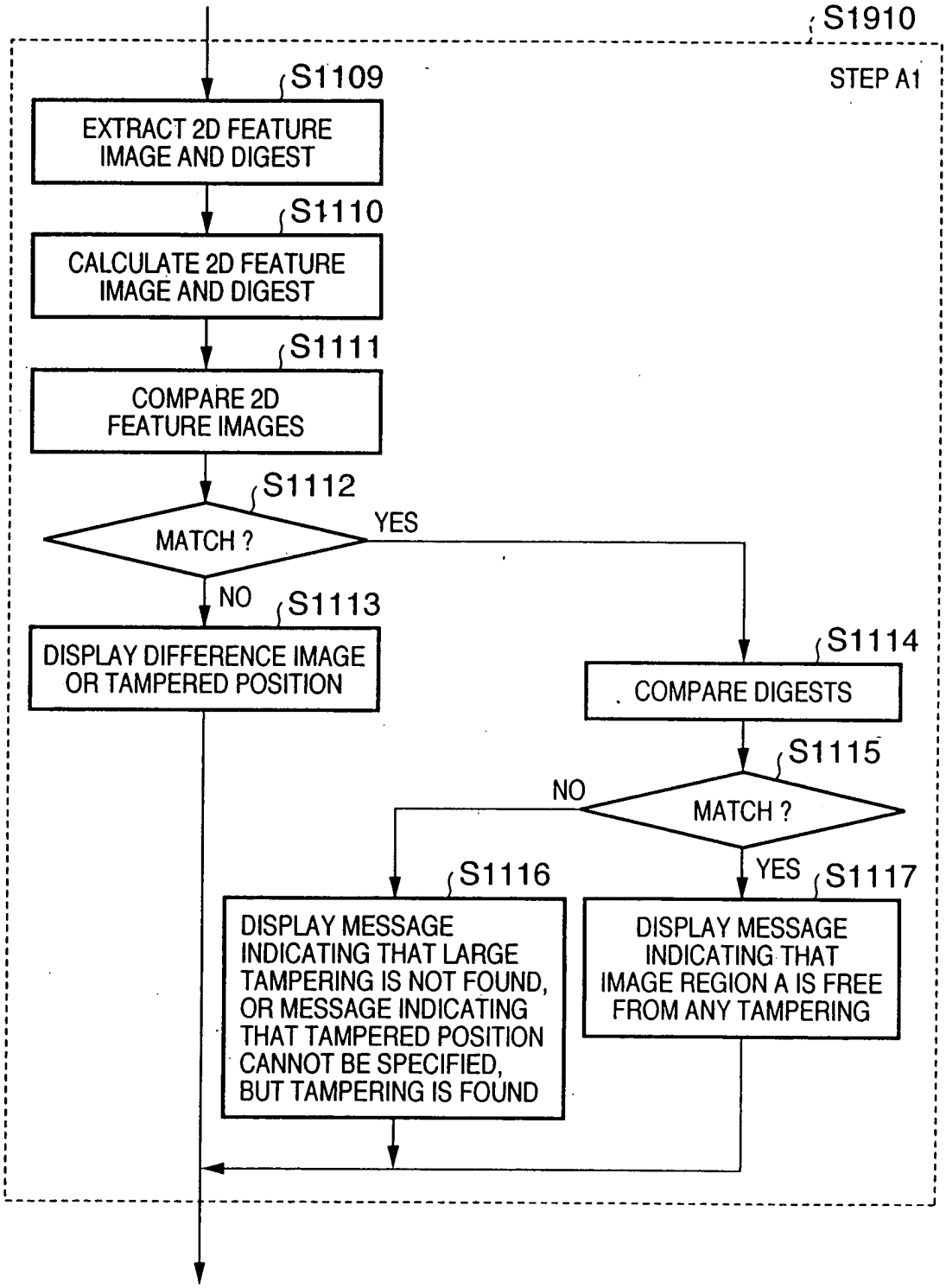

S1910
STEP A1
S1109
EXTRACT 2D FEATURE IMAGE AND DIGEST
S1110
CALCULATE 2D FEATURE IMAGE AND DIGEST
S1111
COMPARE 2D FEATURE IMAGES
S1112
MATCH ?
YES
NO
S1113
DISPLAY DIFFERENCE IMAGE OR TAMPERED POSITION
S1114
COMPARE DIGESTS
S1115
MATCH ?
NO
YES
S1116
DISPLAY MESSAGE INDICATING THAT LARGE TAMPERING IS NOT FOUND, OR MESSAGE INDICATING THAT TAMPERED POSITION CANNOT BE SPECIFIED, BUT TAMPERING IS FOUND
S1117
DISPLAY MESSAGE INDICATING THAT IMAGE REGION A IS FREE FROM ANY TAMPERING

FIG. 21

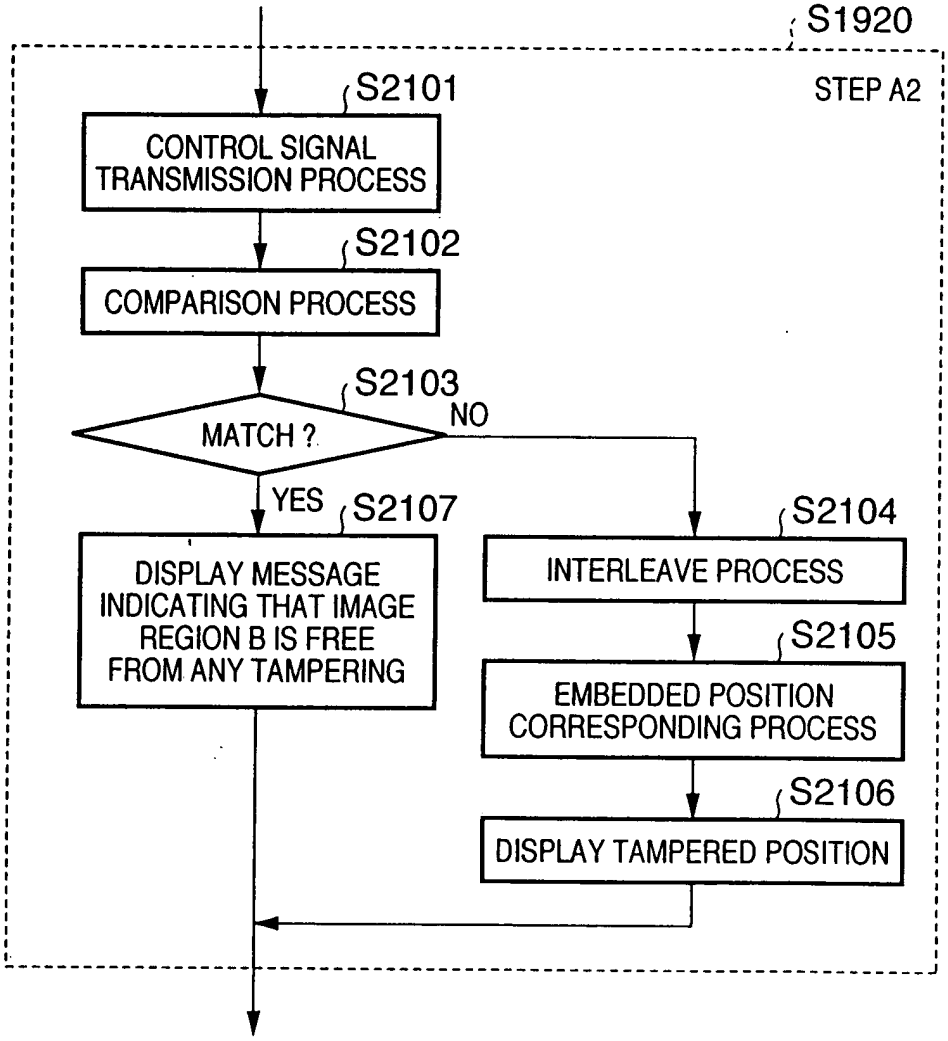
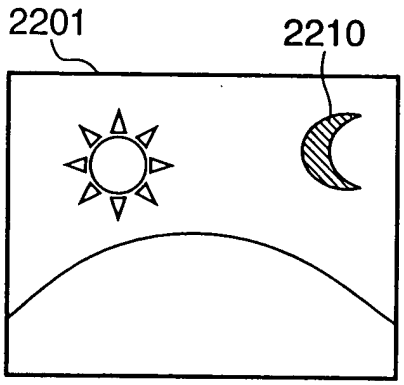
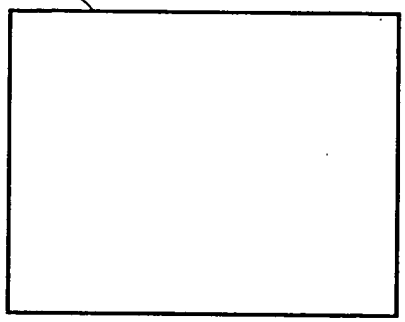

S1920
STEP A2
S2101
CONTROL SIGNAL TRANSMISSION PROCESS
S2102
COMPARISON PROCESS
S2103
MATCH ?
NO
YES
S2107
DISPLAY MESSAGE INDICATING THAT IMAGE REGION B IS FREE FROM ANY TAMPERING
S2104
INTERLEAVE PROCESS
S2105
EMBEDDED POSITION CORRESPONDING PROCESS
S2106
DISPLAY TAMPERED POSITION

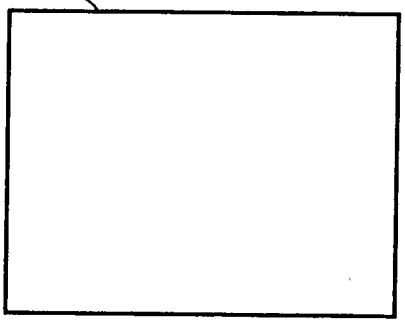
FIG. 22



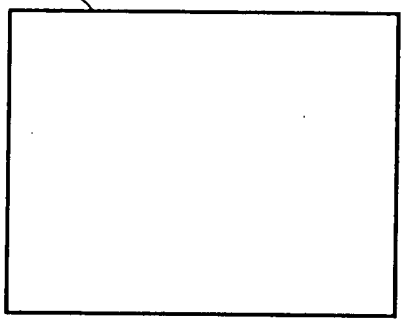
TAMPERED IMAGE
(MULTI-VALUE)



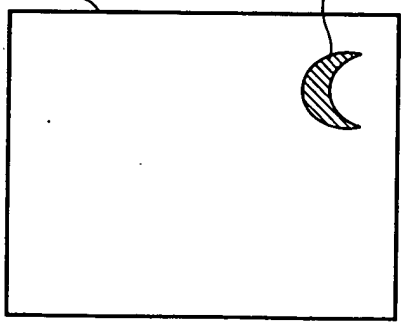
PARTIALLY DESTROYED,
ERROR-CORRECTION ENCODED,
ENCRYPTED WATERMARK INFORMATION



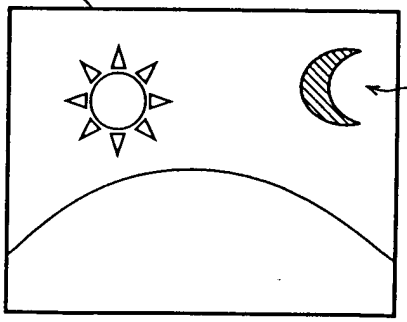
ERROR-CORRECTED,
ERROR-CORRECTION ENCODED,
ENCRYPTED WATERMARK INFORMATION



BIT SEQUENCE FOR SPECIFYING
SECOND TAMPERED POSITION



DIFFERENCE IMAGE INDICATING
TAMPERED POSITION



DISPLAY OF
TAMPERED
POSITION

IMAGE INDICATING TAMPERED POSITION
IN TAMPERED IMAGE (MULTI-VALUE)

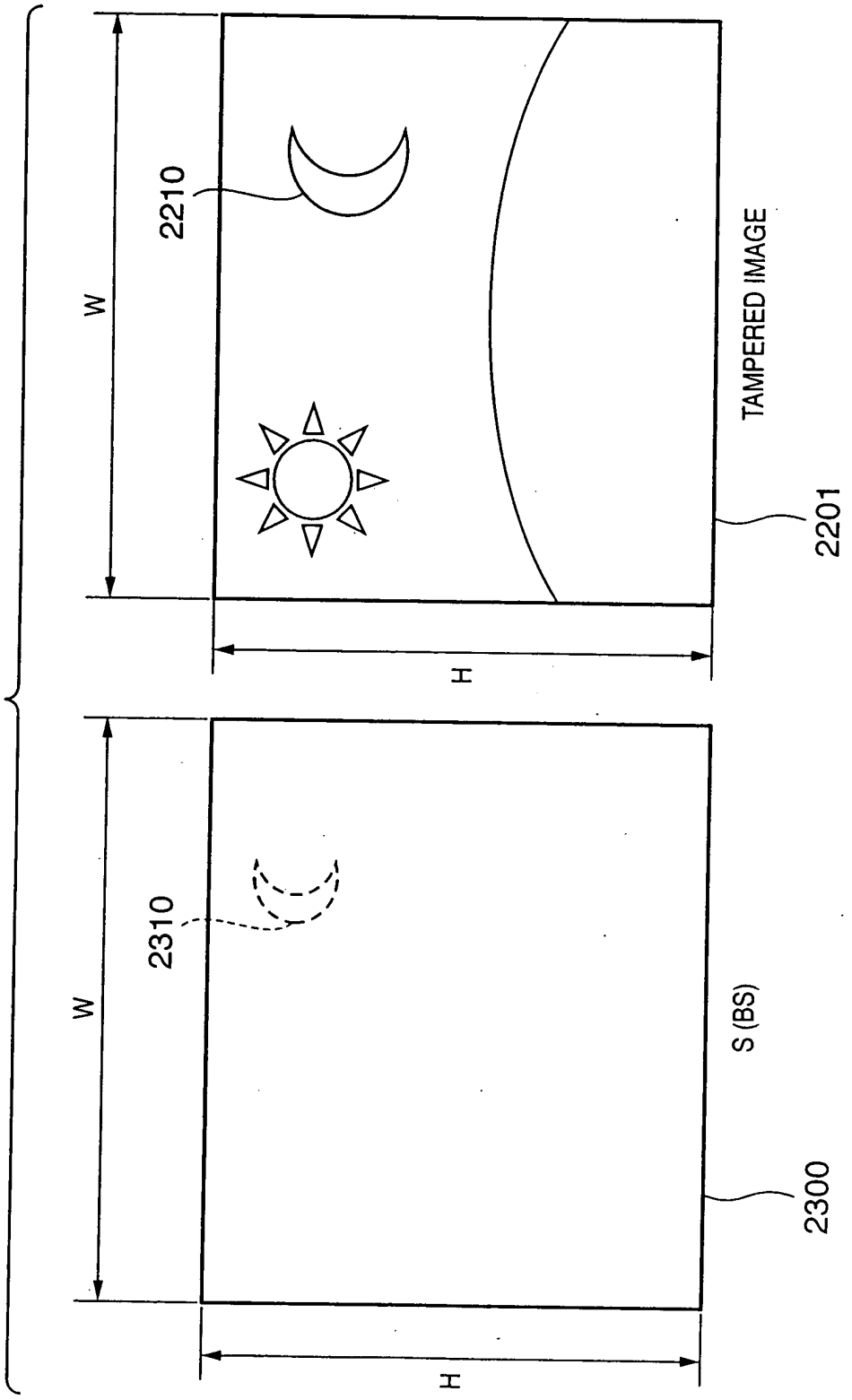



FIG. 23